О БЕЗОПАСНОСТИ И ПРЕДОТВРАЩЕНИИ МОШЕННИЧЕСТВА

Мы хотим быть надежным партнером для наших клиентов и делаем все, что от нас зависит, чтобы сохранить ваши данные в безопасности. Мы благодарны за все сообщения, которые помогают нам сделать наши услуги более безопасными. Сообщения можно передавать по телефону 667 3200 или на электронную почту info@tkmfinants.ee.

В своей деятельности мы придерживаемся следующих принципов безопасности

- ✓ Мы устанавливаем вашу личность в среде самообслуживания карты Partner с помощью надежных цифровых средств аутентификации, к которым относятся Smart-ID, mobiil-ID, ID-карта или банковская ссылка. Нам не нужно знать ни ваших ПИН-кодов, ни идентификаторов пользователей интернет-банком, ни номеров ваших банковских карт.
- ✓ Передача данных шифруется с использованием протокола TLS.
- ✓ Мы просим вас регулярно обновлять ваши данные. Так мы можем обеспечивать безопасность вашего аккаунта, препятствовать злонамеренным действиям, оповещать о подозрительных операциях и тем самым защищать вас от возможного денежного ущерба. Вместе с тем, являясь кредитодателем, мы должны соблюдать законы, которые связаны с противодействием международному отмыванию денег и финансированию терроризма.
- ✓ Мы поможем вам узнать о схемах мошенничества. При совершении действий в интернете будьте внимательны и аккуратны. Мы составили на своем сайте краткий обзор различных ситуаций, которые наиболее часто используются в Эстонии в случаях финансовых мошенничеств. Найдите время для ознакомления с этой информацией, чтобы вы знали, как защитить себя от мошенников.

Самые распространенные финансовые мошенничества

«Банковское мошенничество»

К вам обращаются по электронной почте, СМС, через Messenger или по телефону и представляются работниками TKM Finants AS, Kaubamaja или Selver. Вас могут направить на веб-сайт, который очень похож на сайт карты Partner, и мошенник может спросить у вас, например, номер банковской карты и ее код CVV, ваш идентификатор пользователя в интернет-банке или личный код и ПИН-коды. Также у вас могут спросить информацию об операциях, совершенных с помощью платежных решений Partner Kuukaartи т. п. информацию. После сбора информации, в зависимости от данных, данные могут быть использованы для входа в ваш интернет-банк и осуществления перечислений с вашего счета, для заключения от вашего имени кредитных договоров или также для использования платежных решений Partner Kuukaart в интернет-магазинах и т. д. Также полученная от вас информация может быть использована для того, чтобы предъявить вам от нашего имени счета, но получателем платежа мошенник указывает свой банковский счет.

«Мошенничество со счетом»

Мошенники отправляют вам счет от имени TKM Finants AS за товар или услугу, которые вы не заказывали/покупали. Также может случиться, что счет будет предъявлен за услугу или товар,

которые вы получили в действительности, но банковский счет получателя платежа отличается от нашего. Мошенники надеются, что вы не будете проверять счет и сделаете перечисление.

«Мошенничество с розыгрышем призов»

Мошенники создают от имени известной компании поддельный аккаунт на платформах социальных сетей (Facebook, Instagram, Twitter) и создают пост с содержанием привлекательного розыгрыша призов. Например: Selver разыгрывает покупательскую корзину на 100 евро на целый год или Kaubamaja разыгрывает подарочную карту на 1000 евро.
Также жертве может быть отправлено электронное письмо или сообщение через социальные сети, в котором утверждается, что он выиграл приз, несмотря на то, что он даже не принимал участие ни в какой игре/кампании.
Если жертва кликнет на рекламу, его попросят предоставить персональные данные, совершить платеж, ввести номер банковского счета или банковской карты и т. д. После сбора информации, в зависимости от данных, данные могут быть использованы для входа в ваш интернет-банк и осуществления перечислений с вашего счета, от вашего имени могут заключить кредитные договоры, могут использовать платежные решения Partner Kuukaart и т. д.
Также после нажатия на ссылку на ваше устройство может быть установлена вредоносная программа, которая в дальнейшем будет отслеживать все ваши действия и сохранять ваши персональные данные и финансовую информацию.

«Романтическое мошенничество»

Встреча с мошенником происходит в сети, например, в социальных сетях или на портале знакомств, где мошенник представляется ложным именем. Мошенники очень активно общаются, они преследуют цель быстро вызвать у вас большие и глубокие чувства, чтобы получить контроль над вами. Вскоре после знакомства с вами мошенники попросят вас о финансовой помощи, ссылаясь на такие причины, как внезапная потеря работы, несчастный случай, неудачный бизнес или помощь своему близкому человеку. Финансовая помощь может заключаться, например, также в том, что мошенник попросит вас приобрести кухонную технику или другой товар в Kaubamaja с помощью платежного решения Partner Kuukaart. Если вы этого не сделаете, мошенник может начать угрожать вам, используя для этого ваши интимные разговоры. Такие манипуляции зачастую имеют повторяющийся характер.

Полезные советы

- ✓ Храните ПИН-код платежного лимита Partner Kuukaart в недоступном для других месте. Помните, что кошелек не является безопасным местом для хранения ПИН-кода.
- ✓ Если к вам обращаются по телефону, электронной почте или приложение для общения, представляясь сотрудником какого-либо банка, Kaubamaja, Selver, TKM Finants или в связи с картой Partner, и у вас спрашивают, например, номер банковской карты, пароли, ПИН-коды или иную уязвимую финансовую информацию, незамедлительно прекратите общение и сообщите нам об этом по телефону 667 3200 или адресу электронной почты info@tkmfinants.ee.
- ✓ Если вы подозреваете, что это мошенничество, переспросите, с кем они желают говорить. В случае мошеннических звонков, как правило, звонящий не знает, на чей номер он звонит.
- ✓ Убедитесь, что адрес сайта карты Partner введен в браузер правильно и что вы используете безопасное соединение. На сайте должен быть знак навесного замка, и при нажатии на него должна отражаться информация: «Безопасное подключение» (англ. —

«Connection is secure»). Если браузер оповещает вас о возможных проблемах безопасности или сертификата, воздержитесь от использования сайта.

- ✓ Обновите программное обеспечение как в телефоне, так и в компьютере, а также регулярно осуществляйте обновления защиты.
- ✓ По возможности установите в свои устройства защиту от вирусов.
- ✓ Не разглашайте никому свои идентификационные признаки для входа в интернет-банк, пароли и ПИН-коды для аутентификации. Помните, что ни банки, ни мы никогда не спрашиваем ваших паролей и ПИН-кодов ни по телефону, ни по электронной почте.
- ✓ При использовании mobiil-ID и Smart-ID всегда убеждайтесь, что отображаемый в вашем мобильном телефоне контрольный код соответствует коду, показанному в интернет-банке или мобильном приложении. ПИН-коды mobiil-ID и Smart-ID можно вводить только в соответствующем приложении вашего мобильного телефона. ПИН-коды mobiil-ID и Smart-ID никогда нельзя вводить на сайтах, в том числе в интернет-банке или среде самообслуживания карты Partner!
- ✓ Для входа в среду самообслуживания карты Partner используйте всегда код ПИН1. Если для этого у вас запрашивают код ПИН2, то незамедлительно прервите вход в систему и сообщите нам об этом случае.
- ✓ Будьте осторожны с разглашением личной информации знакомым (особенно интернет-знакомым). Эта информация может быть использована для манипулирования вами.
- ✓ Если это возможно, проверьте информацию о знакомом из сети (например, с помощью Google). Если у вас возникают сомнения в идентичности человека, прекратите общение.
- ✓ Если вы стали жертвой мошенничества, незамедлительно свяжитесь с полицией. Если по просьбе мошенника вы перечислили деньги, сообщите об этом также своему банку. Сообщайте нам о любых случаях, когда у вас просили использовать платежные решения Partner Kuukaart во благо другого человека, или если вы обнаружите, что ваши данные против вашей воли были использованы для заключения договоров Partner Kuukaart.
- ✓ Будьте осторожны с электронными письмами, отправленными с незнакомых адресов, или отправленными с незнакомых номеров СМС. Всегда проверяйте правописание и грамматику — ошибки указывают на мошенническое сообщение. Никогда не открывайте ссылки, отправленные сомнительным электронным письмом или сообщением.
- ✓ С большой осторожностью относитесь к сообщениям, в которых утверждается, что вы что-то выиграли, если знаете, что вы ничего не делали для этого выигрыша. Никогда не открывайте ссылки, отправленные в таких сообщениях.
- ✓ При получении по электронной почте счетов за товары или услуги всегда перепроверяйте, совпадает ли номер банковского счета получателя с номером счета, указанным на официальном сайте поставщика услуг или продавца. Номера счетов TKM Finants AS можно найти в среде самообслуживания карты Partner www.partnerkaart.ee.